AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

Southern District of West Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Subject property located at 259 Sunset Drive, Alderson, WV 24910, and the person of Jack Michael Smith

Case No. 5:20-mj-00053

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Subject property located at 259 Sunset Drive, Alderson, WV 24910, and the person of Jack Michael Smith - Further described in Attachment A.

located in the Southern District of West Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2252A	Possession of child pornography

The application is based on these facts:

See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days: _____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Terrance Taylor, HSI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: October 13, 2020

City and state: Beckley, WV

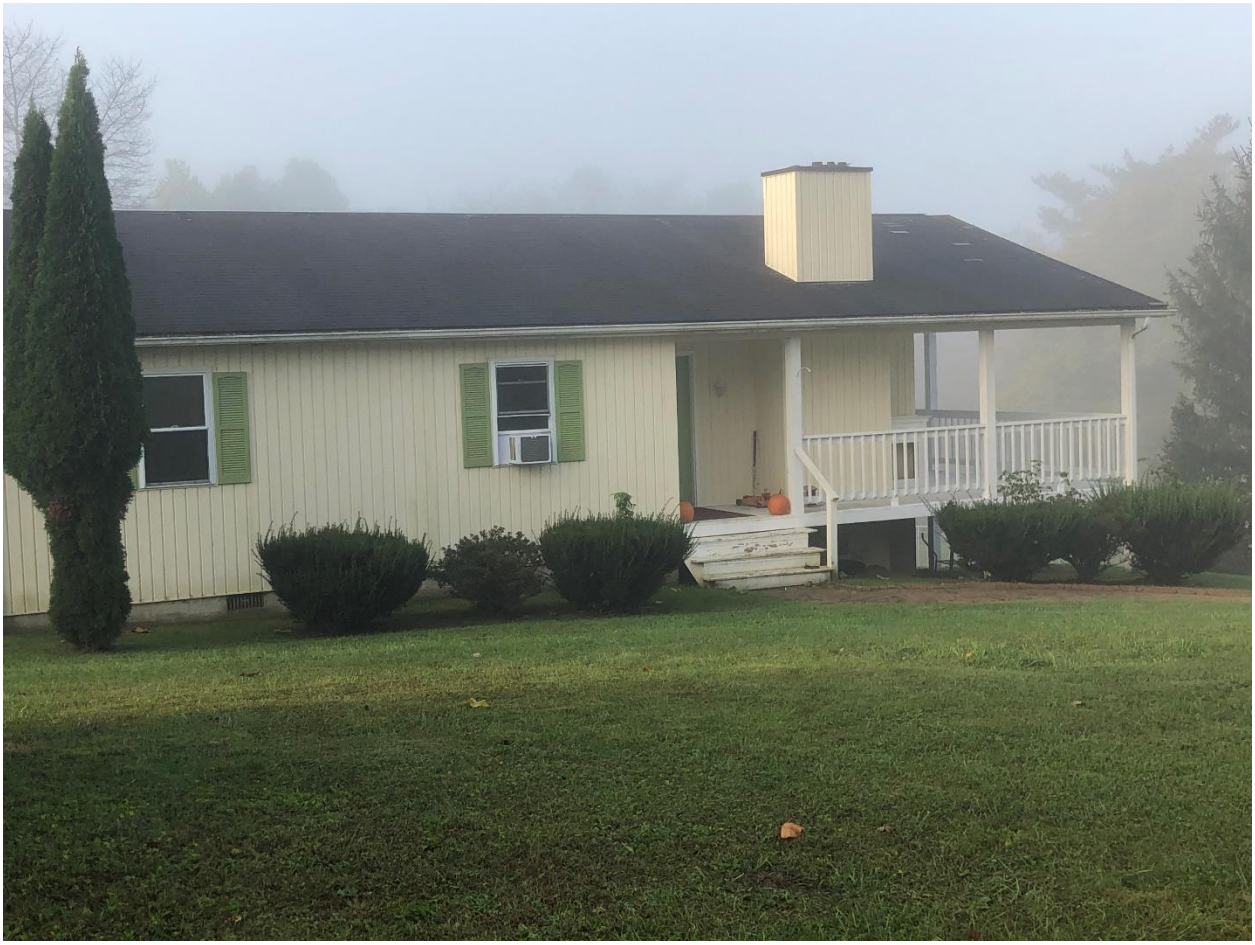
Omar J. Aboulhosn
United States Magistrate Judge
Printed name and title

Print | Save As... | Attach | Reset

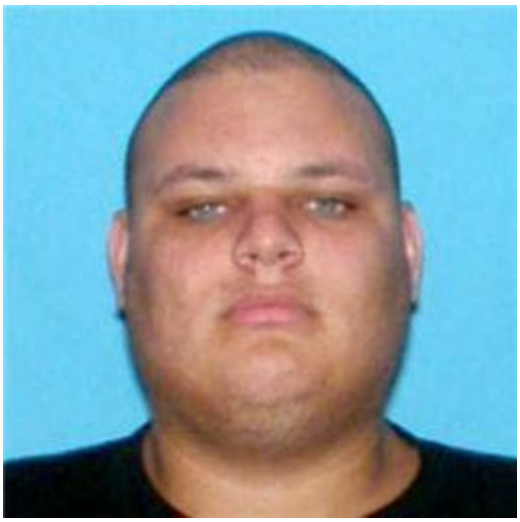
ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The entire property located 259 Sunset Drive, Alderson, WV 24910, including the residential building, any outbuildings, and any appurtenances thereto (the SUBJECT PREMISES), any vehicle(s) located at the SUBJECT PREMISES, and the person of Jack SMITH located at the SUBJECT PREMISES. The SUBJECT PREMISES is more particularly described as a one-story, single-family residence with yellow siding and green shutters. The address number "259" is located on a mailbox in the front yard. A photograph of the property is included below.



A) The person of Jack Michael SMITH, should SMITH be present at the SUBJECT PREMISES at the time the search warrant is executed. A photograph of SMITH is shown below:



ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. 2252A (a)(5)(B) and (b)(2):

1. Computers or storage media used as a means to commit the violations described above, specifically any device belonging to or used by Jack SMITH or where ownership cannot be determined.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

   a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

   b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

   c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, 259 Sunset Drive, Alderson, West Virginia, including utility and telephone bills, mail envelopes, or addressed correspondence;

b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

d. Records and information relating to sexual exploitation of children, including correspondence and communications between users of child pornography and exploitation websites.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to compel Jack SMITH to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

(a) any of the DEVICES found at the PREMISES, and

(b) where the DEVICES are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the DEVICES's security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the PREMISES to provide biometric features, as described in the preceding paragraph, to

access or otherwise unlock any DEVICE. Further, this warrant does not authorize law enforcement personnel to request that Jack SMITH state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

IN THE UNITED STATES DISTRICT COURT
FOR SOUTHERN DISTRICT OF WEST VIRGINIA

IN THE MATTER OF THE SEARCH OF: 259 SUNSET DRIVE, ALDERSON, WEST VIRGINIA 24910, AND THE PERSON OF JACK MICHAEL SMITH LOCATED THEREIN	Case No. 5:20-mj-00053

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Terrance L. Taylor, being duly sworn, do hereby depose and state the following:

I. INTRODUCTION

1. I am a Special Agent (SA) with the U. S. Department of Homeland Security, Homeland Security Investigations ("HSI"). I have been so employed since March 2012. I am currently assigned to the Office of the Resident Agent in Charge HSI Charleston, West Virginia. Since this time, your Affiant has gained experience in conducting investigations involving computers and the procedures that are necessary to retrieve, collect, and preserve electronic evidence. Through your Affiant's training and experience, including on-the-job discussions with other law enforcement agents and cooperating suspects, I am familiar with the operational techniques and organizational structure of child pornography distribution networks and child pornography possessors and their use of computers and other media devices.

2. I am a Special Agent with eighteen years of federal law enforcement experience. Prior to my employment with HSI, your Affiant was a Police Officer for two years in Huntington, West Virginia, a Special Agent with the United States Department of State-Bureau of Diplomatic Security for six years, a Special Agent with the Naval Criminal Investigative Service for two years,

and a Special Agent with the U. S. Department of State-Office of Inspector General (DOS OIG) for two years. I am a graduate of three federal law enforcement academies at the Federal Law Enforcement Training Center (FLETC) and a graduate of the West Virginia State Police Academy. I graduated from the Criminal Investigator Training Program in 2002, and the Immigration and Customs Enforcement Special Agent Training Program in 2012. As part of these programs, I have received extensive training in the areas of law within the jurisdiction of HSI. These areas include laws and regulations pertaining to the importation of various types of merchandise and contraband, prohibited items, money laundering, and various immigration violations. I have more specifically received training in the areas of child pornography and the sexual exploitation and abuse of children. This training includes specialized instruction on how to conduct criminal investigations related to violations of child protection laws pursuant to Title 18, United States Code, Sections 2251, 2252, 2252A, and 2256.

3. As a special agent, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the FLETC, Immigration and Customs Enforcement, as well as everyday work relating to investigations involving the receipt, possession, access with intent to view, production, importation, advertising, and distribution of child pornography that occur in the Southern District of West Virginia. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have obtained search warrants for child pornography offenses, and I have been the case agent or assisted others in numerous investigations involving the sexual exploitation of children. Moreover, I am a federal

law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2252(a)(2)(A) and (B)(2) (receipt or distribution of images, in interstate or foreign commerce, depicting a minor engaging in sexually explicit conduct), 2252A(a)(2) (receipt or distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography), and I am authorized by law to request a search warrant.

II. PURPOSE OF THE AFFIDAVIT

4. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in Attachment A of this Affidavit, including the entire property located at 259 Sunset Drive, Alderson, Greenbrier County, West Virginia (the "SUBJECT PREMISES"), the content of electronic storage devices located therein, any vehicle(s) located at the SUBJECT PREMISES, and the person of Jack Michael SMITH located at the SUBJECT PREMISES, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2)(A) and (a)(5)(B), which items are more specifically described in Attachment B of this Affidavit.

5. This Affidavit is also submitted in support of an application for a search warrant for the person described in Attachment A of this Affidavit, Jack Michael SMITH. As set forth herein, there is probable cause to search the person of SMITH, as described in Attachment A, for the items described in Attachment B, including cell phones and digital storage devices such as thumb drives that can be concealed on the person should SMITH be present in the SUBJECT PREMISES. I believe probable cause exists for the issuance of a warrant to search SMITH, as described in Attachment A, for (1) property that constitutes evidence of a federal criminal offense; (2) contraband, the fruits of a federal crime, or things otherwise criminally possessed; and/or (3)

property designated or intended for use or which is or has been used as the means for committing a federal criminal offense, namely 18 U.S.C. §§ 2252A(a)(2) (receipt or distribution of child pornography) and 2252A(a)(5)(B) (possession of child pornography).

6. The statements in this Affidavit are based in part on information provided by the National Center for Missing and Exploited Children (NCMEC), the HSI Cyber Crimes Center (C3), state and local law enforcement officers, and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations or attempted violations of 18 U.S.C. §§ 2252A(a)(2) and 2252A(a)(5)(B) receipt, distribution, and possession of child pornography are presently located in the SUBJECT PREMISES.

III. STATUTORY AUTHORITY

7. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly receiving or distributing any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; or any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

b. 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing, or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

IV. DEFINITIONS

8. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction

involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. "Cloud storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices

(including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords" and "data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an

IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

i. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

j. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

k. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

l. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

m. "Remote Computing Service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

n. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

o. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

p. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

V. BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

9. On October 15, 2019, Tumblr reported to NCMEC suspected child pornography via Cyber Tipline report numbers 57149768 and 57149821. Tumblr user identified with screen/user name "reapersmith", e-mail address "jmikesmith2000@gmail.com," and associated Internet Protocol (IP) addresses 75.109.17.51, 2601:1c0:8600:5de0:f5aa:1d9b:6415:3e1f, and

173.81.241.5, uploaded eleven child exploitation images of a female child to a Tumblr chat with an unknown individual. The images were uploaded on October 13, 2019, at 00:55:33 EDT.

10. Tumblr captured the uploading of a specific file titled, "9f9c8e168e93c22ffcb77595b11d17bd_tumblr_messaging_pzar0kxU7k1s7o01x_raw.png" on October 13, 2019, with associated IP address 75.109.17.51. This file is an image depicting a nude, pubescent female approximately 11-13 years of age. The female is lying on her back with her legs pulled back and her legs spread open and bare vagina exposed. Semen is depicted on the female's vagina and anus. The female's face is not visible to the viewer. However, ten associated images of the female were also captured by Tumblr in which the female's face and nude, developed breasts are visible to the viewer.

11. The Tumblr chat associated to "reapersmith" details his relationship with the unknown female child. "Reapersmith" claimed to have an ongoing sexual relationship with a 13-year old girl whom he babysat. "Reapersmith" claimed to be a friend of the child's parents. "Reapersmith" claimed to have been molesting the female child since she was three years old.

VI. IDENTIFICATION OF SUBECT PREMISES

12. On October 21, 2019, a subpoena/summons was issued to Yaana Technologies, LLC. regarding IP address 75.109.17.51. A review of the results obtained on November 4, 2019 identified the following account holder and address:

Subscriber Name: Jack SMITH

Service Address: [redacted] Cedar Knoll Drive, Ronceverte, WV

13. In relation to the aforementioned Tumblr Cyber Tipline report, HSI C3 reported that Kik Interactive, Inc., identified a Kik user with screen/user name "grimreaper5150", e-mail

address "jmikesmith2000@gmail.com," and associated Internet Protocol (IP) addresses 166.170.28.83 and 173.81.241.5, uploaded one child exploitation image of a female child to Kik. The image was uploaded on March 22, 2019, at 04:57:25 UTC.

14. Kik captured the uploading of the file through a PhotoDNA hash match on March 22, 2019. This file is an image depicting a nude, prepubescent female approximately 7-10 years of age with brown hair. The female is leaning on a bathtub while wearing handcuffs and ankle bracelets that are connected by a chain. The female's breasts and vagina are exposed in a full-frontal view to the viewer. The female's face is visible to the viewer and her body does not appear to have developed pubic hair or breasts.

15. On October 21, 2019, a subpoena/summons was served to Yaana Technologies, LLC. regarding IP address 173.81.241.5. A review of the records obtained on November 4, 2019 identified the following account holder and address:

Subscriber Name: Alice Clark

Subscriber Address: [redacted] Calhoun Street, Alderson, WV

16. On October 15, 2020, a search of a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses and other information was conducted for Jack Michael SMITH. These records indicated that Alice CLARK is the owner of the residence located at [redacted] Calhoun Street, Alderson, WV. These records also document a grandson of Jack Michael SMITH residing at that address.

17. On October 1, 2020, your Affiant obtained West Virginia Driver's License information from the West Virginia Fusion Center. SMITH's West Virginia Identification Card, #I426144, depicted his photograph, listed his year of birth as 1986, and identified his Social

Security Number. SMITH listed his address as [redacted] Calhoun Street, Alderson, WV. SMITH's Identification card was issued on October 11, 2016.

18. Surveillance of the Calhoun Street residence on or about October 7, 2020, revealed a red Jeep Cherokee, West Virginia registration 62G 225. DMV records indicate the registered owner as Alice CLARK.

19. On or about October 7, 2020, contact was made with Alice CLARK. CLARK advised that her grandson, SMITH, moved out recently and moved in with his girlfriend in Alderson, WV.

20. On or about October 7, 2020, your Affiant obtained SMITH's application for a martial arts studio. The application depicted SMITH's updated residence as 259 Sunset Drive, Alderson, West Virginia (SUBJECT PREMISES). The application further depicted SMITH's email address as jmikesmith2000@gmail.com, his phone number as [redacted]-1252, and his year of birth as 1986. Kimberly CROOKSHANKS was also listed on the application.

21. Surveillance of the SUBJECT PREMISES on or about October 8, 2020, revealed a blue Ford Focus, West Virginia registration 76C 480. This vehicle is registered to Kimberly CROOKSHANKS. Another vehicle located at the SUBJECT PREMISES was a blue Chrysler Sebring, West Virginia registration MAUWAKEE. This vehicle is registered to SMITH.

VII. BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

22. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port

on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with

other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

i. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 250 gigabytes of data, which provides enough space to store thousands of high-

resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

j. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem.[1] Because of the proliferation of commercial services that provide electronic mail service, chat services (*i.e.* "instant messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

k. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of

[1] The File Transfer Protocol (FTP) is a protocol that defines how to transfer files from one computer to another. One example, known as "anonymous FTP," allows users who do not have a login name or password to access certain files from another computer, and copy those files to their own computer.

images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

l. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

m. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

n. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this

information can be intentional (*i.e*. by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally, such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g*., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

VII. CHARACTERISTICS COMMON TO INDIVIDUALS WHO POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

23. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who possess, receive, distribute, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual

arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the

individual "deleted" it.[2]

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. It has long been recognized by professionals dealing with persons involved with child pornography that child pornography has enduring value to those involved in the sexual exploitation of children. Such persons rarely, if ever, dispose of their sexually explicit material. Those materials are often treated as prized possessions. Individuals involved in child pornography almost always maintain their materials in a place that they consider secure and where the materials are readily accessible. Most frequently, these materials are kept within the privacy and security of their own homes. These materials are kept on their person in forms of media storage

[2] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

devices such as thumb drives and cellphones in their pants pockets and on their keychains.

24. Your Affiant believes that given the continuing nature of possession of child pornography and the general character of such offenders as "collectors" and "hoarders," there is probable cause to believe that evidence of violations of federal law, including, but not limited to, 18 U.S.C. §§ 2252A(a)(2) (receipt or distribution of child pornography) and 2252A(a)(5)(B) (possession of child pornography) will be present in the SUBJECT PREMISES, and on the person of SMITH, as described in Attachment A, when the search is conducted. There is probable cause to believe that evidence of the violations of federal law, as described in Attachment B, will be located in the SUBJECT PREMISES and on the person of SMITH, as described in Attachment A. Thus, even if the individual associated with the SUBJECT PREMISES, believed at this time to be SMITH, uses a portable device (such as a mobile phone) to access the internet and child pornography, there is probable cause that evidence of this access will be found in the SUBJECT PREMISES in addition to being on his person.

25. Based on the foregoing, I believe that the user of the internet account that uploaded the twelve images involving children on March 22, 2019, and October 13, 2019, respectively, likely displays characteristics common to individuals who receive, distribute, and possess child pornography. For example, the target of the investigation uploaded eleven images of child pornography to the Tumblr account and uploaded one image of child pornography to the Kik account identified in this Affidavit on two separate occasions. It is probable that the individual, believed at this time to be SMITH, either obtained images of child pornography from other, possibly unidentified, child exploitation websites or from other like-minded individuals who show

characteristics common to individuals who receive, distribute, or possess images of child pornography.

26. As described further in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B), of any device belonging to or used by Jack SMITH, or where ownership cannot be determined. An onsite preview will be conducted of any devices where ownership cannot established.

27. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active

file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

d. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

e. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

28. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or

storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also

indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to distribute or attempt to distribute child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of a crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

29. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data

recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

30. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

31. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require

techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

IX. BIOMETRIC ACCESS TO DEVICES

32. This warrant permits law enforcement to compel Jack SMITH to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices

produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted

Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any DEVICES that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of Jack SMITH to the fingerprint scanner of the DEVICES found at the PREMISES; (2) hold the DEVICES found at the PREMISES in front of the face of Jack SMITH and activate the facial recognition feature; and/or (3) hold the DEVICES found at the PREMISES in front of the face of Jack SMITH and activate the iris recognition feature, for the purpose of attempting to unlock the DEVICES in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel that Jack SMITH state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to compel Jack SMITH to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

VIII. CONCLUSION

33. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

34. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

SPECIAL AGENT TERRANCE L. TAYLOR
DEPARTMENT OF HOMELAND SECURITY
HOMELAND SECURITY INVESTIGATIONS

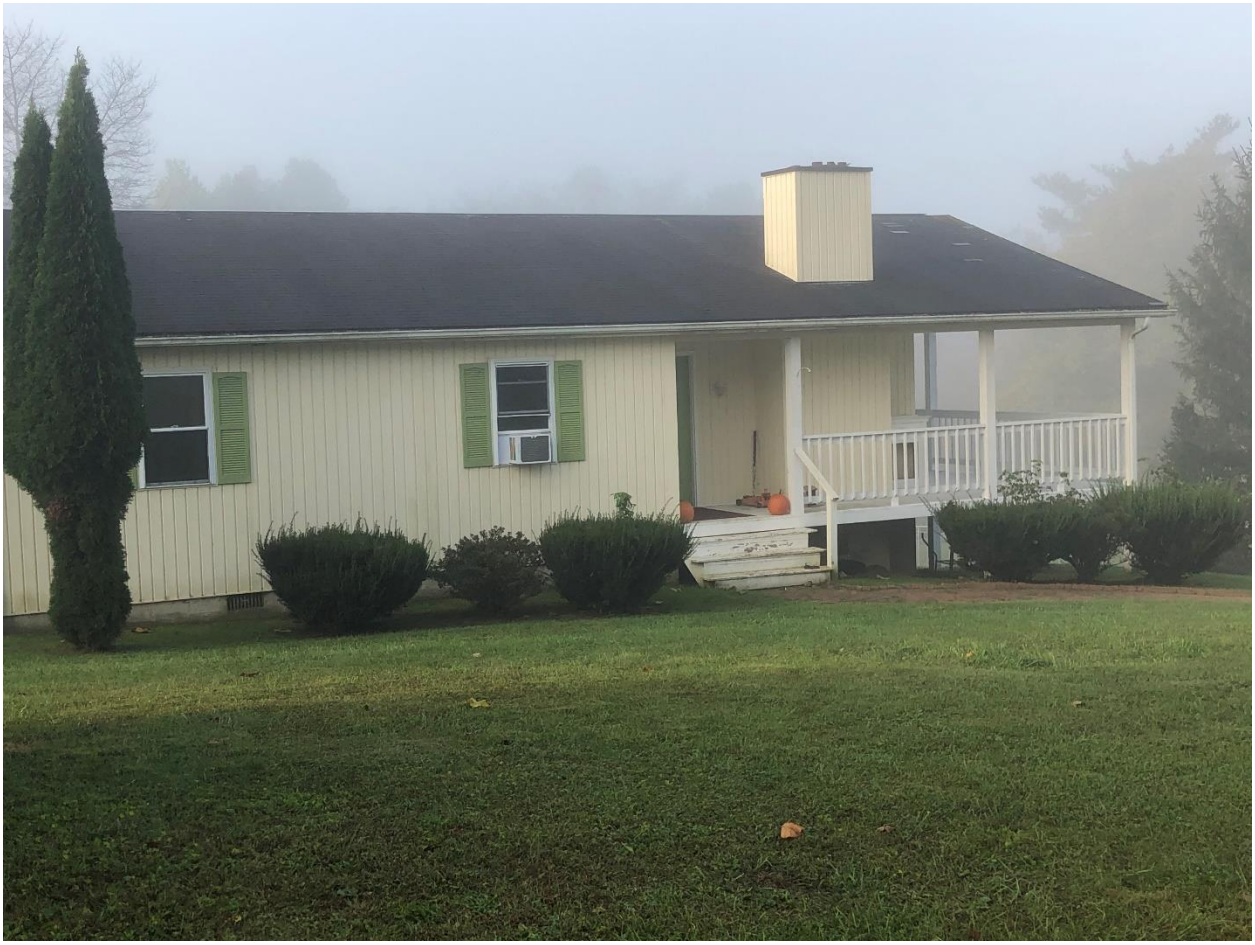
Signed and sworn to by telephonic means on this _____ day of October, 2020:

OMAR J. ABOULHOSN
UNITED STATES MAGISTRATE JUDGE

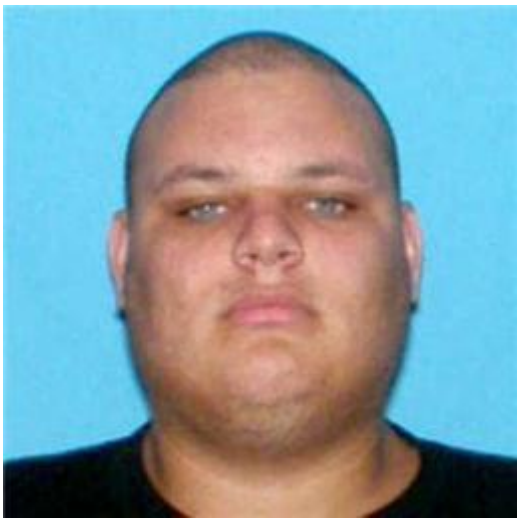
ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The entire property located 259 Sunset Drive, Alderson, WV 24910, including the residential building, any outbuildings, and any appurtenances thereto (the SUBJECT PREMISES), any vehicle(s) located at the SUBJECT PREMISES, and the person of Jack SMITH located at the SUBJECT PREMISES. The SUBJECT PREMISES is more particularly described as a one-story, single-family residence with yellow siding and green shutters. The address number "259" is located on a mailbox in the front yard. A photograph of the property is included below.



A) The person of Jack Michael SMITH, should SMITH be present at the SUBJECT PREMISES at the time the search warrant is executed. A photograph of SMITH is shown below:



ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. 2252A (a)(5)(B) and (b)(2):

1. Computers or storage media used as a means to commit the violations described above, specifically any device belonging to or used by Jack SMITH or where ownership cannot be determined.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

   a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

   b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

   c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, 259 Sunset Drive, Alderson, West Virginia, including utility and telephone bills, mail envelopes, or addressed correspondence;

b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

d. Records and information relating to sexual exploitation of children, including correspondence and communications between users of child pornography and exploitation websites.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to compel Jack SMITH to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

(a) any of the DEVICES found at the PREMISES, and

(b) where the DEVICES are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the DEVICES's security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the PREMISES to provide biometric features, as described in the preceding paragraph, to

access or otherwise unlock any DEVICE. Further, this warrant does not authorize law enforcement personnel to request that Jack SMITH state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.